UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA

Robert Volio, individually and on behalf of all others similarly situated, Plaintiff, v. Rush Street Gaming LLC and Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia, Defendants.	Case No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Robert Volio ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendants Rush Street Gaming LLC ("RSG") and Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia (collectively, "Defendants"), and alleges as follows:

INTRODUCTION

1. This class action arises out of Defendants' failure to properly secure and safeguard the personally identifiable information ("PII") of Plaintiff and other similarly situated current and former employees and customers of Defendants ("Class Members").

2. On or about November 18, 2024, Defendants determined that certain files were unlawfully exfiltrated off their systems ("Data Breach").

3. Defendants failed to mention when they first came to learn of the Data Breach.

4. Moreover, Defendants appear to have been ill-prepared to face the threat of a cyberattack, notwithstanding that such attacks and their resulting harm is imminently foreseeable.

5. The impact to its systems strongly implies that Defendant lacked sufficient cybersecurity incident response and disaster recovery plans, or that the plans it had were not sufficiently tests through the use of tabletop exercises, as is the industry norm.

6. Plaintiff brings this action on behalf of all persons whose PII was compromised because of Defendants' failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) timely warn Plaintiff and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure its network containing such PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal statutes.

7. Defendants have not provided affected persons or the public any information regarding how the Data Breach occurred or what it is doing to prevent another such incident in the future.

8. Moreover, Defendants' significantly delayed investigation and notification of the Data Breach strongly implies that Defendant lacked a serious and tested cybersecurity incident response plan, which is a core aspect of any reasonable, industry standard cybersecurity program.

9. By failing to implement cybersecurity safeguards, Defendants blatantly disregarded the rights of Plaintiff and the Class Members, including their right to control how their PII is disseminated.

10. Because Defendants still maintain Plaintiff's and Class Members' PII on their information systems, they have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

11. Plaintiff brings this action to hold Defendants accountable for their failure to properly safeguard Plaintiff's and the proposed Class Members' PII that they collected, including

by requiring Defendants to provide monetary compensation to Plaintiff and the proposed Class Members for this egregious invasion of their privacy, for allowing their PII to fall into the hands of cybercriminals and identity thieves, to provide them with compensation and the means to protect themselves against the significant increase in identity theft and financial fraud they must now combat, and to require Defendants to implement the reasonable, industry standard cybersecurity safeguards necessary to protect the PII of Plaintiff and the proposed Class Members that Defendants still has in their possession.

12. Indeed, by collecting Plaintiff's and Class Members' PII, Defendants had a duty under the common law to implement reasonable, industry standard cybersecurity safeguards, but failed to implement them, including by failing to implement reasonable policies that would have allowed them to timely respond to this Data Breach, and likely including the failure to train their employees to defend against phishing emails, the failure to employ multi-factor authentication, and at least the failure to encrypt Plaintiff's and Class Members' PII, given that it was accessed by unauthorized third-parties in unencrypted form. Moreover, the timeline, as explained above, strongly implies that Defendants lacked appropriate logging, monitoring, and alerts systems as well as appropriate cybersecurity incident response and disaster recovery/continuity plans.

13. Because of Defendants' failures, Plaintiff and Class Members have suffered concrete injuries, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) experiencing an increase in spam calls, texts, and/or emails; (vi) statutory damages; (vii) nominal damages; and (viii) the continued and substantially increased risk of identity theft and financial fraud.

JURISDICTION AND VENUE

14. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendants, and (4) there are more than 100 proposed Class members.

15. This Court has personal jurisdiction over Defendants because Defendant Sugarhouse HSP Gaming, L.P. maintains a principal place of business in this District, Defendants conduct substantial business in this District, and the events giving rise to Plaintiff's claims arise out of Defendants' contacts with this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia is a resident and citizen of this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

PARTIES

17. Plaintiff Robert Volio is, and at all relevant times was, a resident and citizen of Philadelphia, Pennsylvania.

18. Defendant Rush Street Gaming LLC is a limited liability company registered in the State of Delaware, and upon information and belief, is headquartered in Illinois.

19. Defendant Sugarhouse HSP Gaming, L.P. d/b/a Rivers Casino Philadelphia is a Delaware Limited Partnership with its principal place of business located at 1001 North Delaware Avenue, Philadelphia, Pennsylvania 19123.

FACTUAL ALLEGATIONS

Defendants' Business

20. Defendants own and operate Rivers Casino Philadelphia.[1]

21. Defendant RSG claims it "takes reasonable measures to help protect information about you from loss, theft, misuse and unauthorized access, disclosure, alteration and destructions."[2]

22. Defendant RSG further represents it is "based in the United States and the information we collect is governed by U.S. law." [3]

23. Plaintiff and Class members are employees and customers of Defendants.

24. Plaintiff and Class members provided certain Personally Identifying Information ("PII") to Defendants.

25. As a sophisticated gaming company with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendants are well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII in its possession.

The Data Breach

26. According to Defendants, it was "determined that an unauthorized actor accessed and/or took certain files stored on [Defendants'] computer servers."[4]

[1] https://www.riverscasino.com/philadelphia/ (last visited Jan. 4, 2025)
[2] https://www.riverscasino.com/philadelphia/privacy-policy (last visited Jan. 4, 2025)
[3] *Id.*
[4] *See* Data Breach Notification Letter, attached hereto as ***Exhibit A***.

27. Defendants claim that "on November 18, 2024, we determined that one or more file(s) contained your name and one or more of the following: Social Security number, and/or bank account information used for direct deposit."[5]

28. Defendants began notifying affected persons on or about December 30, 2024.[6]

29. Defendants' letter also offered free credit monitoring services to those potentially impacted by the breach.

30. Defendants did not state why they were unable to prevent the Data Breach or which security feature failed.

31. Defendants did not state why they did not contact affected persons about the breach sooner than one month after discovering the breach.

32. Defendants failed to prevent the data breach because they did not adhere to commonly accepted security standards and failed to detect that their databases were subject to a security breach.

Injuries to Plaintiff and the Class

33. Shortly after December 30, 2024, Plaintiff received a breach notification from Defendants indicating that his PII was compromised during the Data Breach.[7] According to the notification letter, the Data Breach exposed Plaintiff's name, Social Security number, and bank account information.

34. Since the Data Breach, Plaintiff has received a significant increase in phishing emails and spam texts.

[5] *Id.*
[6] *Id.*
[7] *See* Ex. A.

35. In response to the Data Breach, Plaintiff has spent significantly more time checking his bank and credit card statements than he did prior to the Data Breach.

36. Plaintiff is very concerned about the theft of his PII and has and will continue to spend substantial amounts of time and energy monitoring his credit status.

37. As a direct and proximate result of Defendants' actions and omissions in failing to protect Plaintiff's PII, Plaintiff and the Class have been damaged.

38. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

39. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[8]

40. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic

[8] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

41. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value and/or use of their PII entrusted to Defendant, and loss of privacy.

The Value of PII

42. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

43. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[9]

44. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[10]

45. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[11] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers

[9] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.
[10] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.
[11] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[12]

Industry Standards for Data Security

46. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, and Capital One, Defendants are, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of their systems being breached.

47. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

[12] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

48. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[13] and protection of PII[14] which includes basic security standards applicable to all types of businesses.

49. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

[13] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[14] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

50. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[15]

51. Because Defendants were entrusted with consumers' PII, they had, and have, a duty to consumers to keep their PII secure.

52. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII to companies such as Defendants, that their PII will be safeguarded.

53. Nonetheless, Defendants failed to prevent the Data Breach. Had Defendants properly maintained and adequately protected their systems, they could have prevented the Data Breach.

CLASS ACTION ALLEGATIONS

54. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

55. The proposed Class is defined as follows:

[15] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

Nationwide Class: All persons whose PII was maintained on Defendants' servers and compromised in the Data Breach.

56. Plaintiff reserves the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

57. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, the number can be readily identified through Defendants' records.

58. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendants owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendants breached that duty or those duties;

c. Whether Defendants failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendants was satisfactory to protect customer and employee information as compared to industry standards;

e. Whether Defendants misrepresented or failed to provide adequate information to customers and employees regarding the type of security practices used;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiff's and the Class's PII secure and prevent loss or misuse of that PII;

g. Whether Defendants acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII;

h. Whether Defendants' conduct was intentional, willful, or negligent;

i. Whether Defendants violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendants' conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendants' conduct.

59. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendants relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

60. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff has retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

61. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendants owed a duty to Plaintiff and the Class and whether Defendants breached their duties predominate over individual questions such as measurement of economic damages.

62. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendants' actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits

of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

63. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

64. The Class may be certified pursuant to Rule 23(b)(2) because Defendants have acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

65. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

66. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/ NEGLIGENCE PER SE
(on behalf of the Class)

67. Plaintiff hereby incorporates by reference paragraphs 1 through 66 as though fully set forth herein.

68. Defendants owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of their systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class

members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendants knew that they were more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

69. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

70. Defendants' violations of Section 5 of the FTC Act constitute negligence per se.

71. Defendants breached the aforementioned duties when they failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

72. Defendants further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit their processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII within their possession, custody, and control.

73. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

74. Defendants admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the breach.

75. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

76. By engaging in the forgoing acts and omissions, Defendants committed the common law tort of negligence. For all the reasons stated above, Defendants' conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

77. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class, their PII would not have been compromised.

78. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendants have an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendants are liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendants are also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendants' negligence. Defendants are also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated.

COUNT II
INVASION OF PRIVACY
(on behalf of the Class)

79. Plaintiff hereby incorporates by reference paragraphs 1 through 66 as though fully set forth herein.

80. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

81. Defendants invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII, as set forth above.

82. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII was disclosed without prior written authorization from Plaintiff and the Class.

83. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII to Defendants privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

84. As a direct and proximate result of Defendants' above acts, Plaintiff's and the Class's PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

85. Defendants are guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII with a willful and conscious disregard of their right to privacy.

86. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause Plaintiff and the Class great and irreparable injury in that the PII maintained by Defendants can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendants may freely treat Plaintiff's and the Class's PII with sub-standard and insufficient protections.

COUNT III
UNJUST ENRICHMENT
(on behalf of the Class)

87. Plaintiff hereby incorporates by reference paragraphs 1 through 66 as though fully set forth herein.

88. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendants and that was ultimately compromised in the data breach.

89. Defendants, by way of their acts and omissions, knowingly and deliberately enriched themselves by saving the costs they reasonably should have expended on security measures to secure Plaintiff's and the Class's PII.

90. Defendants also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

91. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendants instead consciously and opportunistically calculated to increase their own profits at the expense of Plaintiff and the Class. Nevertheless, Defendants continued to obtain the benefits conferred on them by

Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendants were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

92. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendants' decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

93. Thus, Defendants engaged in opportunistic conduct in spite of their duties to Plaintiff and the Class, wherein they profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits they derived as a consequence of their conduct.

94. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically, the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendants as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: January 4, 2025

Respectfully submitted,

/s/Kenneth J. Grunfeld
Kenneth J. Grunfeld
Jeff Ostrow*
KOPELOWITZ OSTROW P.A
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 525-4100
grunfeld@kolawyers.com
ostrow@kolawyers.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and Proposed Class

Pro Hac Vice Application Forthcoming*